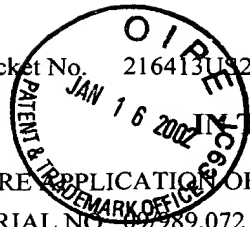


2137#4

Docket No. 216413US2S/btm



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Asahiko YAMADA, et al.

GAU: 2131

SERIAL NO. 69989,072

EXAMINER:

FILED: November 21, 2001

FOR: SYSTEM, METHOD, AND PROGRAM FOR ENSURING ORIGINALITY

RECEIVED
JAN 17 2002
Technology Center 2100

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number [US App No], filed [US App Dt], is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

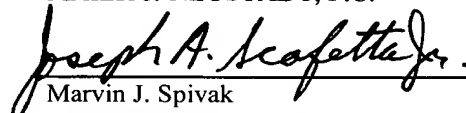
<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
JAPAN	2000-356239	November 22, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
 - ☐ are submitted herewith
 - ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.


Marvin J. Spivak

Registration No. 24,913

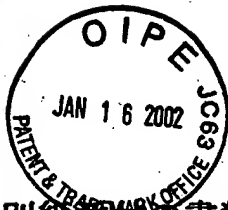
Joseph A. Scafetta, Jr.
Registration No. 26,803



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

09/989,072



日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2000年11月22日

出 願 番 号
Application Number:

特願2000-356239

出 願 人
Applicant(s):

株式会社東芝

Technology Center 2100

JAN 17 2002

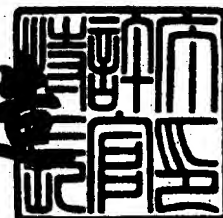
RECEIVED

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年11月 9日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2001-3099064

【書類名】 特許願

【整理番号】 A000006737

【提出日】 平成12年11月22日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/00

【発明の名称】 原本性保証システム及びプログラム

【請求項の数】 4

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中事業所内

 【氏名】 山田 朝彦

【発明者】

 【住所又は居所】 東京都府中市東芝町1番地 株式会社東芝府中事業所内

 【氏名】 原嶋 秀次

【特許出願人】

 【識別番号】 000003078

 【氏名又は名称】 株式会社 東芝

【代理人】

 【識別番号】 100058479

 【弁理士】

 【氏名又は名称】 鈴江 武彦

 【電話番号】 03-3502-3181

【選任した代理人】

 【識別番号】 100084618

 【弁理士】

 【氏名又は名称】 村松 貞男

【選任した代理人】

 【識別番号】 100068814

 【弁理士】

 【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 原本性保証システム及びプログラム

【特許請求の範囲】

【請求項 1】 電子化データに対するユーザ装置の電子署名に対し、第三者機関装置の発行した日時情報を付与し、これら電子署名と日時情報の組に対して第三者機関装置の電子署名を施すことにより、前記電子化データの原本性を保証することを特徴とする原本性保証システム。

【請求項 2】 電子化データに対するユーザ装置の電子署名に対し、第三者機関装置の電子署名を施すことにより、前記電子化データの原本性を保証する原本性保証システムに関し、前記ユーザ装置に用いられるプログラムであって、

前記第 1 のユーザ装置のコンピュータを、

操作者の操作により、電子化データを作成する手段、

前記電子化データのうち、前記原本性の保証の対象となる電子化データに対して電子署名を生成する手段、

前記電子署名を前記第三者機関装置に送信する手段、

として機能させるためのプログラム。

【請求項 3】 電子化データに対するユーザ装置の電子署名に対し、自己の電子署名を施して前記電子化データの原本性を保証するための原本性保証ポータルサービスを提供する第三者機関装置と、前記第三者機関装置から提供される原本性保証ポータルサービスをネットワークを介して利用するユーザ装置とからなる原本性保証システムであって、

前記第三者機関装置は、

前記ユーザ装置が登録されるテーブルと、

前記テーブルに登録されたユーザ装置に対し、予め前記原本性保証ポータルサービスを利用するためのプログラムを提供する手段と、

前記プログラムを用いてアクセスされたとき、前記アクセスしてきたユーザ装置のアクセス権限を前記テーブルを参照して確認する手段と、

前記アクセス権限の確認されたユーザ装置に対し、前記原本性保証ポータルサービスの利用を許可する手段と、

を備えたことを特徴とする原本性保証システム。

【請求項 4】 請求項 3 に記載の原本性保証システムにおいて、
前記ユーザ装置は、

前記第三者機関装置による電子署名と前記電子化データとを送信する際に、送信先の候補として、前記テーブルの登録内容を前記第三者機関装置に要求する手段と、

前記要求に対する応答に基づき、前記テーブルの登録内容をリスト表示する手段と、

を備えたことを特徴とする原本性保証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、信頼できる第三者機関を介して文書の原本性を保証し得る原本性保証システム及びプログラムに係り、特に、第三者機関やネットワークにかかる負荷を低減し得る原本性保証システム及びプログラムに関する。

【0002】

【従来の技術】

一般に、電子化された電子化文書をインターネットを介して交換するサービスは、電子化文書の原本性保証が困難である性質上、電子化文書の原本性が重要視される分野には普及が妨げられて来ている。

【0003】

しかしながら、近年、暗号技術の発展とともに、原本性を保証する技術が実現され始めたことに伴い、原本性保証技術を実装した原本性保証サービスが使用され始めている。

【0004】

この種の原本性保証サービスは、信頼できる第三者機関 T T P (Trusted Third Party) の計算機に電子化文書を送信することにより、第三者機関 T T P に原本性を保証させる方式を基本的な技術としている。なお、以下の明細書中、第三者機関 T T P は、組織そのものではなく、第三者機関 T T P に運営されるサーバ

装置等の計算機を意味する。

【 0 0 0 5 】

【発明が解決しようとする課題】

しかしながら以上のような原本性保証システムでは、第三者機関 T T P を経由して電子化文書を交換するため、第三者機関 T T P への電子化文書の送信が集中した場合、第三者機関 T T P や、第三者機関 T T P までの間のネットワークに対し、負荷がかかる問題がある。

【 0 0 0 6 】

本発明は上記実情を考慮してなされたもので、第三者機関やその間のネットワークにかかる負荷を低減し得る原本性保証システム及びプログラムを提供することを目的とする。

【 0 0 0 7 】

【課題を解決するための手段】

第 1 の発明は、電子化データに対するユーザ装置の電子署名に対し、第三者機関装置の発行した時刻情報を付与し、これら電子署名と時刻情報の組に対して第三者機関装置の電子署名を施すことにより、前記電子化データの原本性を保証する原本性保証システムである。

【 0 0 0 8 】

これにより、電子化データの原本性保証の際に、第三者機関装置には電子化データが送信されないので、第三者機関装置にアクセスが集中した際にも、第三者機関やその間のネットワークにかかる負荷を低減させることができる。

【 0 0 0 9 】

第 2 の発明は、電子化データに対するユーザ装置の電子署名に対し、第三者機関装置の電子署名を施すことにより、前記電子化データの原本性を保証する原本性保証システムに関し、前記ユーザ装置に用いられるプログラムであって、前記第 1 のユーザ装置のコンピュータを、操作者の操作により、電子化データを作成する手段、前記電子化データのうち、前記原本性の保証の対象となる電子化データに対して電子署名を生成する手段、前記電子署名を前記第三者機関装置に送信する手段、として機能させるためのプログラムである。

これにより、第1の発明と同様の作用を奏することができる。

【0010】

第3の発明は、電子化データに対するユーザ装置の電子署名に対し、自己の電子署名を施して前記電子化データの原本性を保証するための原本性保証ポータルサービスを提供する第三者機関装置と、前記第三者機関装置から提供される原本性保証ポータルサービスをネットワークを介して利用するユーザ装置とからなる原本性保証システムであって、前記第三者機関装置としては、前記ユーザ装置が登録されるテーブルと、前記テーブルに登録されたユーザ装置に対し、予め前記原本性保証ポータルサービスを利用するためのプログラムを提供する手段と、前記プログラムを用いてアクセスされたとき、前記アクセスしてきたユーザ装置のアクセス権限を前記テーブルを参照して確認する手段と、前記アクセス権限の確認されたユーザ装置に対し、前記原本性保証ポータルサービスの利用を許可する手段と、を備えた原本性保証システムである。

これにより、第1の発明と同様な作用を奏する原本性保証システムをネットワークを介したポータルサービスとして実現することができる。

【0011】

第4の発明は、第3の発明の原本性保証システムにおいて、前記ユーザ装置としては、前記第三者機関装置による電子署名と前記電子化データとを送信する際に、送信先の候補として、前記テーブルの登録内容を前記第三者機関装置に要求する手段と、前記要求に対する応答に基づき、前記テーブルの登録内容をリスト表示する手段と、を備えた原本性保証システムである。

これにより、第3の発明の作用に加え、原本性保証のされた電子化データを送信する際に、送信先の選択を容易に行なうことができる。

【0012】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照しながら説明する。なお、以下の各実施形態は、公開鍵暗号技術に基づく例であり、第1のユーザ装置UA、第2のユーザUB、第三者機関TTPのそれぞれは、自己の公開鍵ペア及び公開鍵証明書を持ち、且つ他者の公開鍵証明書を持っていることを前提とする。

【0013】

(第1の実施形態)

図1は本発明の第1の実施形態に係る原本性保証システムの構成を示す模式図である。この原本性保証システムは、第1のユーザ装置UA、第2のユーザ装置UB及び第三者機関TTPから構成されている。なお、第1及び第2のユーザ装置UA、UBは、合計2台以上の不特定多数の台数のうち、任意の2台を例示したものである。

【0014】

ここで、第1及び第2のユーザ装置UA、UBは、互いに同一構成であるため、第1又は第2のユーザ装置UA/UBを例に挙げて述べる。なお、ユーザ装置UAの説明は、添字のAをBに置換すると、ユーザ装置UBの説明に置換される。逆も同様である。

【0015】

ユーザ装置UAは、第三者装置TTPへの発行要求とその結果の送信に関する発行要求処理部10Aと、他のユーザ装置UBからの受信処理とその通知処理に関する受信処理部20Aと、第三者装置TTPの検索に関するDB検索部30Aとを備えている。また、各部10A～30A、10B～30Bは、それぞれハードウェア及び/又はソフトウェアにより実現可能となっている。ソフトウェアにより実現される場合は、例えば記憶媒体又はネットワークから各部10A～30A、10B～30Bの機能を実現するためのプログラムが予めインストールされた構成となる。

【0016】

発行要求処理部10Aは、記憶部11A、文書入力部12A、署名部13A、発行要求部14A、応答受信部15A及びデータ送信部16Aを備えている。

【0017】

記憶部11Aは、自装置UAの識別情報Aと、自装置UAの公開鍵ペア及び公開鍵証明書と、他装置UB、TTPの公開鍵証明書と、文書入力部12から入力される電子化文書Dと、電子化文書の識別情報 $ID_{A,D}$ と、署名部13により作成された電子署名 $S_A(D)$ と、第三者装置TTPに作成された識別情報 ID_{TTP}

,D、登録日時 $\text{date}_{\text{TTP},D}$ 、電子署名 $S_{\text{TTP}}(\text{ID}_{\text{TTP},D}, S_A(D), \text{date}_{\text{TTP},D})$ とが記憶されるものである。

【0018】

なお、記憶内容の添字のAは、ユーザ装置UAにより作成されたことを示し（例、 $\text{ID}_{A,D}$ 、 $S_A(D)$ ）、記憶内容の添字のTTPは、第三者機関TTPにより作成されたことを示す（例、 $\text{ID}_{\text{TTP},D}$ 、 $\text{date}_{\text{TTP},D}$ 、 $S_{\text{TTP}}(\dots略\dots)$ ）。また、添字のDは、対応する電子化文書Dを示しているので、電子化文書の識別情報 $\text{ID}_{A,D}$ 又は $\text{ID}_{\text{TTP},D}$ としてもよい。また、電子化データとしての電子化文書Dは、文字列からなる文章のみの電子化された文書データに限らず、数表等のデータ又は画像データを含む文書、あるいはこれらの組合せからなる文書でもよく、そのデータ形式及びデータ量は任意のものが使用可能となっている。例えば音声データを含む文書としてもよく、また少ないデータ量であってもよい。

【0019】

文書入力部12Aは、操作者の操作により、電子化文書Dを作成、修正又は編集し、得られた電子化文書Dを記憶部11Aに書込む機能をもっている。

【0020】

署名部13Aは、操作者の操作により、記憶部11A内の対象となる電子化文書Dに対し、自己の秘密鍵を用いて電子署名 $S_A(D)$ を生成する機能と、生成した電子署名 $S_A(D)$ を記憶部11Aに書込む機能とをもっている。

【0021】

発行要求部14Aは、記憶部11Aの内容に基づいて原本性保証データの発行要求を作成する機能と、この発行要求を第三者機関TTPに送信する機能とをもっている。

【0022】

ここで、発行要求は、例えば、要求元（ユーザ装置UA）を示す要求者情報A、電子化文書Dのユーザ装置UAによる電子署名 $S_A(D)$ 、ユーザ装置UAにおける電子化文書Dの識別情報 $\text{ID}_{A,D}$ を含んでいる。すなわち、発行要求は、 $\{A, S_A(D), \text{ID}_{A,D}\}$ からなるデータである。なお、識別情報 $\text{ID}_{A,D}$ は、省略してもよいが、使用されることが処理効率向上の観点から望ましい。

【0023】

応答受信部15Aは、第三者機関TTPから受けた応答データを記憶部11Aに書込む機能をもっている。

【0024】

データ送信部16Aは、操作者の操作又は応答受信部15Aからの制御により、記憶部11Aを参照し、識別情報 $ID_{A,D}$ により特定される電子化文書Dと、応答データから $ID_{A,D}$ を除いてA、 $S_A(D)$ を付加したデータ(=要求側登録データ)とを含む保証済みデータ $\{D, A, S_A(D), ID_{TTP,D}, date_{TTP,D}, S_{TTP}(ID_{TTP,D}, S_A(D), date_{A,D})\}$ をユーザ装置UBに送信する機能をもっている。

【0025】

次に、受信処理部20A、20Bについて説明する。なお、後述する動作説明中では、ユーザ装置UBの受信処理部20Bの動作が述べられるので、混乱を避けるため、ここではユーザ装置UBの受信処理部20Bを例に挙げて説明する。

【0026】

ユーザ装置UBの受信処理部20Bは、改ざん検証部21B、保証確認部22B、受信通知部23B及び確認部24Bを備えている。

【0027】

改ざん検証部21Bは、他のユーザ装置UAから保証済みデータを受けると、保証済みデータ内の識別情報Aに対応する公開鍵証明書を用いて電子署名 $S_A(D)$ を用いて、電子化文書Dの改ざんの有無を検証する機能をもっている。

【0028】

保証確認部22Bは、改ざん検証部21Bによる検証の結果、電子化文書Dに改ざんが無いとき、記憶部11B内の第三者機関TTPの公開鍵証明書を用いて原本性保証データ $S_{TTP}(ID_{TTP,D}, S_A(D), date_{A,D})$ を復号し、復号結果とデータ $S_A(D)$ 、 $ID_{TTP,D}$ 、 $date_{TTP,D}$ とを比較することにより、第三者機関TTPにより原本性が保証された旨を確認する機能をもっている。なお、原本性保証の確認は、改ざんの有無の検証よりも前に行なっても良い。

【0029】

受信通知部 23 B は、改ざん検証部 21 B による改ざん無しの検証と保証確認部 22 B による原本性保証の確認とが完了した後、受信否認防止のための受信通知を作成し、この受信通知 {B、 $ID_{TTP,D}$ 、 $date_{B,D}$ 、 $S_B(S_A(D), date_{B,D})$ } を第三者機関 TTP に送信する機能をもっている。

【0030】

受信通知は、例えば、受信者（ユーザ装置 UB）の識別情報 B、第三者機関 TTP が電子化文書 D に付与した識別情報 $ID_{TTP,D}$ 、ユーザ装置 UB での受信日時 $date_{B,D}$ 、ユーザ装置 UB の受信を証明（受信否認を防止）するための情報 $S_B(S_A(D), date_{B,D})$ を含んでいる。

【0031】

確認部 24 B は、第三者機関 TTP から受信確認を受信すると、 $ID_{TTP,D}$ をキーにして、ユーザ装置 UA から受信した電子化文書 D を検索し、受信通知を第三者機関 TTP が正しく処理できた旨を確認する機能をもっている。

【0032】

受信確認は、例えば、第三者機関 TTP が電子化文書 D に付与した識別情報 $ID_{TTP,D}$ 、B の A からの受信日時 $date_{B,D}$ 、ユーザ装置 UB からの受信通知を証明する情報 $S_{TTP}(S_B(D), date_{B,D})$ を含んでいる。なお、受信日時 $date_{B,D}$ は、ユーザ装置 UB が保存する前提であれば省略してもよい。

【0033】

DB 検索部 30 A は、操作者の操作により、識別情報 $ID_{TTP,D}$ をキーにして第三者機関 TTP の原本性保証 DB を検索し、その登録内容を入手する機能をもっている。

【0034】

一方、第三者機関 TTP は、原本性保証 DB (data base) 40、要求側登録部 41 及び受信側登録部 42 を備えている。

【0035】

原本性保証 DB 40 は、要求側登録部 41 及び受信側登録部 42 により、要求側登録データ { $ID_{TTP,D}$ 、A、 $S_A(D)$ 、 $date_{TTP,D}$ 、 $S_{TTP}(ID_{TTP,D}, S_A(D), date_{A,D})$ } 及び受信側登録データ {B、 $date_{B,D}$ 、 $S_B(S_A(D), da$

$te_{B,D}$ } が識別情報 $ID_{TTP,D}$ をキーにして登録されるものであり、登録内容が各ユーザ装置 U_A 、 U_B の DB 検索部 30 により検索可能となっている。

【0036】

要求側登録部 41 は、ユーザ装置 U_A から発行要求を受けると、この発行要求に基づいて要求側登録データ $\{ID_{TTP,D}, A, S_A(D), date_{TTP,D}, S_{TTP}(ID_{TTP,D}, S_A(D), date_{A,D})\}$ を作成する機能と、作成した要求側登録データを原本性保証 DB に登録する機能と、登録した要求側登録データから $A, S_A(D)$ を除いて $ID_{A,D}$ を付加した応答データ $\{ID_{A,D}, ID_{TTP,D}, date_{TTP,D}, S_{TTP}(ID_{TTP,D}, S_A(D), date_{A,D})\}$ をユーザ装置 U_A に送信する機能とをもっている。

【0037】

ここで、要求側登録データは、例えば、第三者機関 TTP における電子化文書 D の識別情報 $ID_{TTP,D}$ 、要求者（ユーザ装置 U_A ）の識別情報 A 、要求者による電子署名 $S_A(D)$ 、第三者機関 TTP による原本性保証の処理の日時 $date_{TTP,D}$ と、これら $ID_{TTP,D}, S_A(D), date_{A,D}$ を接続した接続データに対する第三者機関 TTP の電子署名としての原本性保証データ $S_{TTP}(ID_{TTP,D}, S_A(D), date_{A,D})$ を含んでいる。すなわち、要求側登録データは、 $\{ID_{TTP,D}, A, S_A(D), date_{TTP,D}, S_{TTP}(ID_{TTP,D}, S_A(D), date_{A,D})\}$ である。

【0038】

受信側登録部 42 は、ユーザ装置 U_B から受信通知を受けると、この受信通知及び原本性保証 DB 中の $ID_{TTP,D}$ に基づいて、受信側登録データ $\{B, date_{B,D}, S_B(S_A(D), date_{B,D})\}$ を識別情報 $ID_{TTP,D}$ に対応付けて追加的に原本性保証 DB に登録する機能と、この登録の後、受信確認 $\{ID_{TTP,D}, date_{B,D}, S_{TTP}(S_B(D), date_{B,D})\}$ をユーザ装置 U_B に送信する機能とをもっている。

【0039】

次に、以上のように構成された原本性保証システムの動作を図 2 の模式図及び図 3 のフローチャートを用いて説明する。なお、図 2 の模式図は、ユーザ装置 U

Aを送信側とし、ユーザ装置UBを受信側としたときの各ユーザ装置UA、UBにおいて必要な機能ブロックのみを図示しており、送信側にとっての受信処理部20Aや受信側にとっての発行要求処理部10Bは夫々図示を省略している。

【0040】

さてユーザ装置UAにおいては、文書入力部12Aが、操作者の操作により、電子化文書Dを作成、修正又は編集し、得られた電子化文書Dを記憶部11Aに書込んだとする。

【0041】

ここで、ユーザ装置UAにおいては、電子化文書の原本性保証が必要な場合、ユーザ装置UBに文書を送信する前に、操作者の操作により、署名部13Aが、記憶部11A内の対象となる電子化文書Dに対し、自己の秘密鍵を用いて電子署名SA(D)を生成し、この電子署名SA(D)を記憶部11Aに書込む。

【0042】

また、発行要求部14Aが、記憶部11Aの内容に基づいて電子化文書Dの原本性保証データの発行要求{A、SA(D)、IDA,D}を作成し、得られた発行要求を第三者機関TTPに送信する(ST1)。

【0043】

第三者機関TTPでは、発行要求を受けると、要求側登録部41が、この発行要求に基づいて要求側登録データ{IDTTP,D、A、SA(D)、dateTTP,D、STTP(IDTTP,D、SA(D)、dateA,D)}を作成し、得られた要求側登録データを原本性保証DB40に登録する(ST2)。

【0044】

次に、要求側登録部41は、ユーザ装置UAに対し、要求側登録データからA、SA(D)を除いてIDA,Dを付加した応答データ{IDA,D、IDTTP,D、dateTTP,D、STTP(IDTTP,D、SA(D)、dateA,D)}をユーザ装置UAに送信する(ST3)。なお、応答データとしては、IDA,Dに代えて、SA(D)を用いてもよい。

【0045】

ユーザ装置UAでは、応答データを受けると、応答受信部15Aがこの応答デ

ータを記憶部11Aに書込む。また、データ送信部16Aが、操作者の操作又は応答受信部15Aからの制御により、記憶部11Aを参照し、識別情報 $ID_{A,D}$ により特定される電子化文書Dと、応答データから $ID_{A,D}$ を除いてA、 $S_A(D)$ を付加したデータ(=要求側登録データ)とを含む保証済みデータ{D、A、 $S_A(D)$ 、 $ID_{TTP,D}$ 、 $date_{TTP,D}$ 、 $S_{TTP}(ID_{TTP,D}$ 、 $S_A(D)$ 、 $date_{A,D}$)}をユーザ装置UBに送信する(ST4)。なお、電子化文書Dは必要により暗号化してもよい。

【0046】

ユーザ装置UBでは、保証済みデータを受けると、改ざん検証部21Bが、保証済みデータ内の識別情報Aに対応する公開鍵証明書を用いて電子署名 $S_A(D)$ を用いて、電子化文書Dの改ざんの有無を検証する。

【0047】

ここで、電子化文書Dに改ざんが無いとき、ユーザ装置UBでは、保証確認部22Bが、第三者機関TTPの公開鍵証明書を用いて原本性保証データ $S_{TTP}(ID_{TTP,D}$ 、 $S_A(D)$ 、 $date_{A,D}$)を復号し、復号結果とデータ $S_A(D)$ 、 $ID_{TTP,D}$ 、 $date_{TTP,D}$ とを比較することにより、第三者機関TTPが原本性を保証したことを確認する。

【0048】

さて、原本性保証の確認の後、ユーザ装置UBでは、受信通知部23Bが、受信否認防止のための受信通知を作成し、この受信通知{B、 $ID_{TTP,D}$ 、 $date_{B,D}$ 、 $S_B(S_A(D)$ 、 $date_{B,D})$ }を第三者機関TTPに送信する(ST5)。

【0049】

第三者機関TTPでは、受信通知を受けると、受信側登録部42が原本性保証DB中の $ID_{TTP,D}$ に基づいて、受信側登録データ{B、 $date_{B,D}$ 、 $S_B(S_A(D)$ 、 $date_{B,D})$ }を識別情報 $ID_{TTP,D}$ に対応付けて追加的に原本性保証DBに登録する(ST6)。

【0050】

しかる後、第三者機関TTPでは、受信側登録部42が受信確認{ $ID_{TTP,D}$ 、 $date_{B,D}$ 、 $S_{TTP}(S_B(D)$ 、 $date_{B,D})$ }をユーザ装置UBに送信する(ST

7)。

【0051】

ユーザ装置UBでは、受信確認を受信すると、確認部24Bが、ID_{TTP,D}をキーにして、ユーザ装置UAから受信した電子化文書Dを検索し、受信通知を第三者機関TTPが正しく処理できた旨を確認する。

【0052】

以上により、ユーザ装置UAに関し、ユーザ装置UBに対する電子化文書の原本性保証と受信否認防止の処理が完了する。

【0053】

以後、ユーザ装置UAがユーザ装置UBの受信を確認したい場合、例えば第三者機関TTPの提供するWWWサービスなどにより、ユーザ装置UA内のDB検索部30AがID_{TTP,D}をキーにして原本性保証DBを検索することにより、原本性保証及び／又は受信を確認することができる。

【0054】

また、この後、必要により、ユーザ装置UAとユーザ装置UBとの役割を交替し、ユーザ装置UBが作成した電子化文書D'に関し、前述同様に、電子化文書D'の原本性保証と、ユーザ装置UAに対する受信否認防止との処理をそれぞれ行なってもよい。すなわち、第1及び第2のユーザ装置UA、UBは、電子化文書の交換により取引等を行なう場合、電子化文書を授受する毎に、互いに役割を交替して原本性保証と受信否認防止を行なうようにしてもよい。

【0055】

上述したように本実施形態によれば、電子化文書Dの原本性保証の際に、第三者機関TTPには電子化文書Dが送信されず、Dよりも情報の少ない電子署名が送信されるので、第三者機関TTPにアクセスが集中した際の第三者機関又はその間のネットワークにかかる負荷を低減させることができる。

【0056】

また、原本性保証DB40に要求側登録データ及び受信側登録データを登録するので、各DB検索部30A、30Bは、後日(ST7の後)あるいは処理途中(例、ST4とST5との間)でも必要により、原本性保証DB40の登録内容

を確認することができる。

【0057】

また、この確認により何らかの立証を行なうことができる。例えば、登録日時 $\text{date}_{\text{TTP},D}$ と、受信日時 $\text{date}_{B,D}$ との差を見ることにより、ユーザ装置 U_A の処理の遅れの有無を立証することができる。

【0058】

(第2の実施形態)

図4は本発明の第2の実施形態に係る原本性保証ポータルサービスの構成を示す模式図である。この原本性保証ポータルサービスは、契約により、第1の実施形態の機能を実現するプログラムを第三者機関 TTP が各ユーザ装置 U_A 、 U_B に提供して実施可能とする方式である。

【0059】

このユーザ装置 U_A 、 U_B に提供されるプログラムは、前述した発行要求処理部 $10A$ 、 $10B$ 、受信処理部 $20A$ 、 $20B$ 及び DB 検索部 $30A$ 、 $30B$ の機能を実現するための、発行要求プログラム $10A^*$ 、 $10B^*$ 、受信処理プログラム $20A^*$ 、 $20B^*$ 、 DB 検索プログラム $30A^*$ 、 $30B^*$ と、送信先の選択処理を実現するための選択プログラム $50A^*$ 、 $50B^*$ とである。なお、この選択プログラム $50A^*$ 、 $50B^*$ は、発行要求処理部 $10A$ 、 $10B$ に関するプログラム $10A^*$ 、 $10B^*$ に組み込まれている。

【0060】

なお、契約の際に、各契約者の各ユーザ装置 U_A 、 U_B は、自装置 U_A 、 U_B の識別情報 A 、 B 、自装置 U_A 、 U_B の公開鍵証明書 P_A 、 P_B 、自装置 U_A 、 U_B のアドレス情報 ADR_A 、 ADR_B 及び自装置 U_A 、 U_B のデータ通信プロトコル (例、 smtp 、 $\text{http}(s)$ 、 $\text{ftp}(s)$) を第三者機関 TTP に提供することを前提とする。

【0061】

第三者機関 TTP は、図5に示すように、これらの提供された情報を各ユーザ装置 U_A 、 U_B 毎にテーブル60に記憶しており、各ユーザ装置 U_A 、 U_B からの要求により、テーブル60の内容を契約者の一覧として要求元のユーザ装置 U

A, UBに提供する機能をもっている。

【0062】

また、契約の後、クライアント装置としての各ユーザ装置UA, UBは、他のユーザ装置UB, UAから文書やデータを受信可能なように、サーバ装置としての第三者機関TTPにログイン可能な状態にあることを前提とする。

【0063】

すなわち、契約の後、各ユーザ装置UA, UBは、図6(a), (b)に示すように、少なくとも第三者機関TTPの識別情報TTPと公開鍵証明書 P_{TTP} とアドレス情報 ADR_{TTP} とデータ通信プロトコルとをテーブルTA, TBに保持し、適宜、他のユーザ装置UB, UAの識別情報B, Aと公開鍵証明書 P_B , P_A とアドレス情報 ADR_B , ADR_A とデータ通信プロトコルとをもテーブルTA, TBに保持した状態にある。

【0064】

一方、第三者機関TTPは、テーブル60を参照して各ユーザ装置UA, UBのアクセス権限を確認可能な状態にあり、アクセス権限の確認されたユーザ装置に対し、原本性保証ポータルサービスの利用を許可する機能をもっている。

【0065】

次に、以上のように構成された原本性保証ポータルサービスの動作を説明する。

【0066】

原本性保証ポータルサービスでは、図7に示すように、第三者機関TTPに対し、前述したステップST1～ST4に対応する登録サービスPS1と、前述したステップST5～ST7に対応する受信確認サービスPS2と、前述したDB検索部30A, 30BによるDB検索に対応する原本性確認サービスPS3とが選択的に実行要求可能となっている。但し、各サービスの実行は、第三者機関TTPがテーブル60を参照し、実行要求したユーザ装置のアクセス権限を確認した後である。

【0067】

例えばユーザ装置UAでは登録サービスPS1を選択すると、第三者機関TT

Pによるアクセス権限の確認により、登録サービスPS1の利用が許可された後、前述したステップST1～ST3に相当する処理が第三者機関TTPとの間で実行される。この処理が完了した後、ユーザ装置UAでは、送信先の選択プログラム50A*が起動され、送信先の選択処理が実行される。

【0068】

ユーザ装置UAでは、この選択処理の実行に伴い、テーブル60に登録された契約者の一覧を第三者機関TTPに要求し、その応答に基づいて、第三者機関TTPと契約中の契約者（例、企業、個人）の一覧を表示する。

【0069】

ここで、ユーザ装置UAの操作者が一覧内の契約者を送信先として選択すると、送信先のユーザ装置UBに対し、所定のデータ通信プロトコルが起動されてユーザ装置UBに送信可能な状態となる。

【0070】

例えばデータ通信プロトコルがsmtpの場合、メイラが起動され送信先のアドレスがユーザ装置UBのアドレスで埋められる。http(s)の場合、送信先のユーザ装置UBのホームページが表示される。ftp(s)の場合、ftp(s)クライアントが立ち上がって送信先のユーザ装置UBに接続される。

【0071】

ユーザ装置UAは、前述したステップST4で送信する保証済みデータを作成し、保証済みデータを選択したデータ通信プロトコルによりユーザ装置UBに送信する。これにより、登録サービスPS1が完了する。

【0072】

受信側のユーザ装置UBは、受信確認サービスPS2を選択すると、第三者機関TTPによるアクセス権限の確認の後、前述したステップST5～ST7に相当する処理を第三者機関TTPと協調しながら自動処理する。自動処理の後、受信確認サービスPS2が完了する。

【0073】

これにより、第1の実施形態と同様に、原本性保証と受信否認防止とを実現することができる。

【0074】

また、ユーザ装置UAは、原本性確認サービスPS3を選択すると、第三者機関TTPによるアクセス権限の確認の後、電子化文書Dの識別情報IDTP,Dを第三者機関TTPに対して提示し、原本性保証DB40から電子署名SA(D)を取り寄せる処理と、この電子署名SA(D)に基づいて、電子化文書Dの原本性を確認する処理とを実行する。これにより、原本性確認サービスPS3が完了する。

【0075】

上述したように本実施形態によれば、第1の実施形態と同様の作用効果をもつ原本性保証サービスを、ネットワークを介したポータルサービスとして実現することができる。また、原本性保証のされた電子化文書を送信する際に、送信先の選択を容易に行なうことができる。

【0076】

なお、上記実施形態に記載した手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピーディスク、ハードディスクなど）、光ディスク（CD-ROM、DVDなど）、光磁気ディスク（MO）、半導体メモリなどの記憶媒体に格納して頒布することもできる。

【0077】

また、この記憶媒体としては、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【0078】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行しても良い。

【0079】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0080】

また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0081】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0082】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0083】

なお、本願発明は、上記各実施形態に限定されるものでなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態は可能な限り適宜組み合わせて実施してもよく、その場合、組み合わされた効果が得られる。さらに、上記各実施形態には種々の段階の発明が含まれており、開示される複数の構成要件における適宜な組み合わせにより種々の発明が抽出され得る。例えば実施形態に示される全構成要件から幾つかの構成要件が省略されることで発明が抽出された場合には、その抽出された発明を実施する場合には省略部分が周知慣用技術で適宜補われるものである。

【0084】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0085】

【発明の効果】

以上説明したように本発明によれば、第三者機関やその間のネットワークにかかる負荷を低減させることができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態に係る原本性保証システムの構成を示す模式図

【図 2】

同実施形態における原本性保証システムの動作を説明するための模式図

【図 3】

同実施形態における動作を説明するためのフローチャート

【図 4】

本発明の第 2 の実施形態に係る原本性保証ポータルサービスの構成を示す模式図

【図 5】

同実施形態における第三者機関側のテーブルの内容を示す模式図

【図 6】

同実施形態におけるユーザ装置側のテーブルの内容を示す模式図

【図 7】

同実施形態における動作を説明するための模式図

【符号の説明】

U A, U B …ユーザ装置

T T P …第三者機関

1 0 A, 1 0 B …発行要求処理部

1 0 A *, 1 0 B * …発行要求プログラム

1 1 A, 1 1 B …記憶部

1 2 A, 1 2 B …文書入力部

1 3 A, 1 3 B …署名部

1 4 A, 1 4 B …発行要求部

1 5 A, 1 5 B …応答受信部

1 6 A, 1 6 B …データ送信部

2 0 A, 2 0 B …受信処理部

2 0 A *, 2 0 B * …受信処理プログラム

2 1 A, 2 1 B …改ざん検証部

2 2 A, 2 2 B …保証確認部

2 3 A, 2 3 B …受信通知部

2 4 A, 2 4 B …確認部

3 0 A, 3 0 B …DB 検索部

3 0 A *, 3 0 B * …DB 検索プログラム

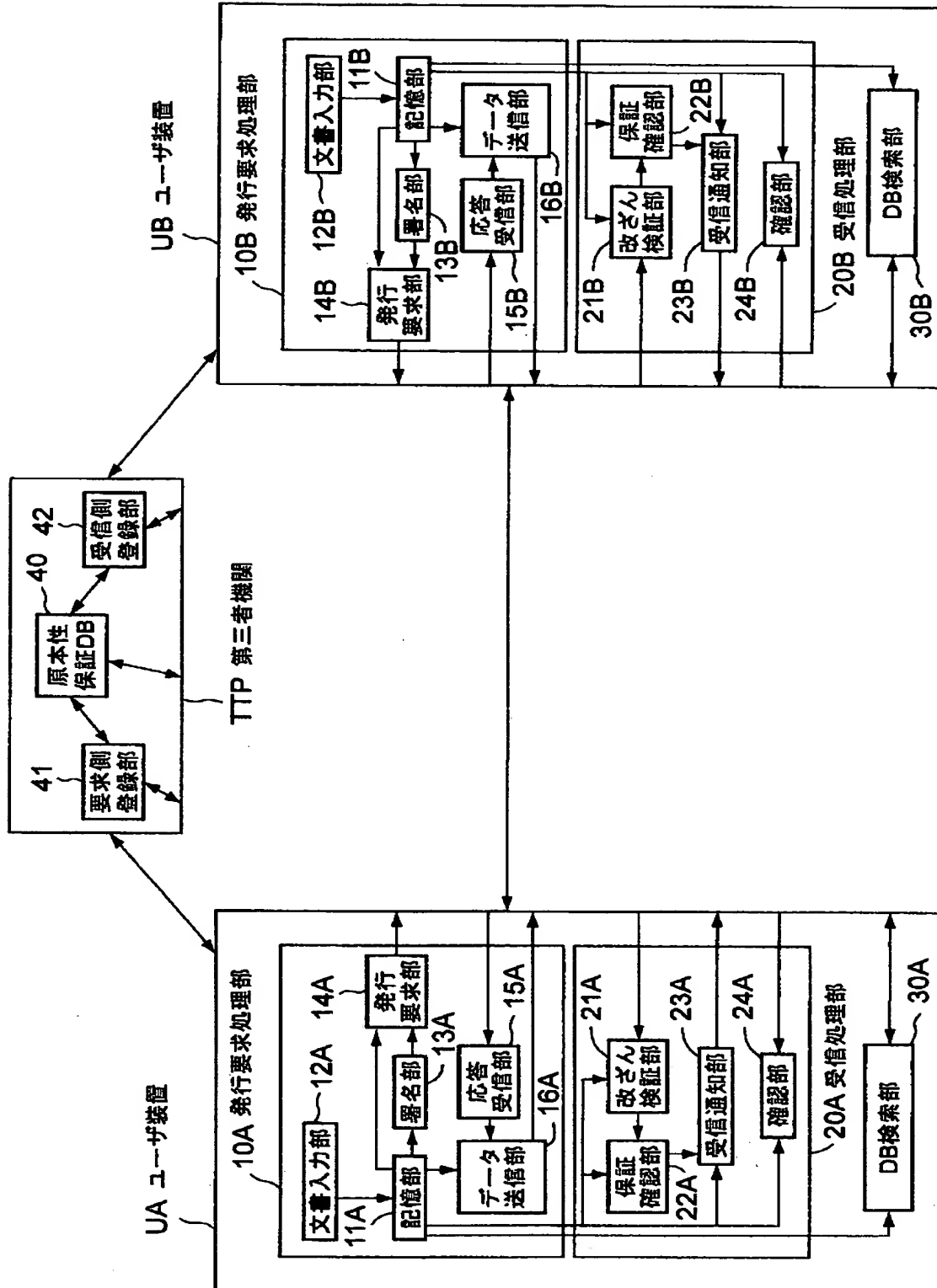
5 0 A *, 5 0 B * …選択プログラム

6 0, T A, T B …テーブル

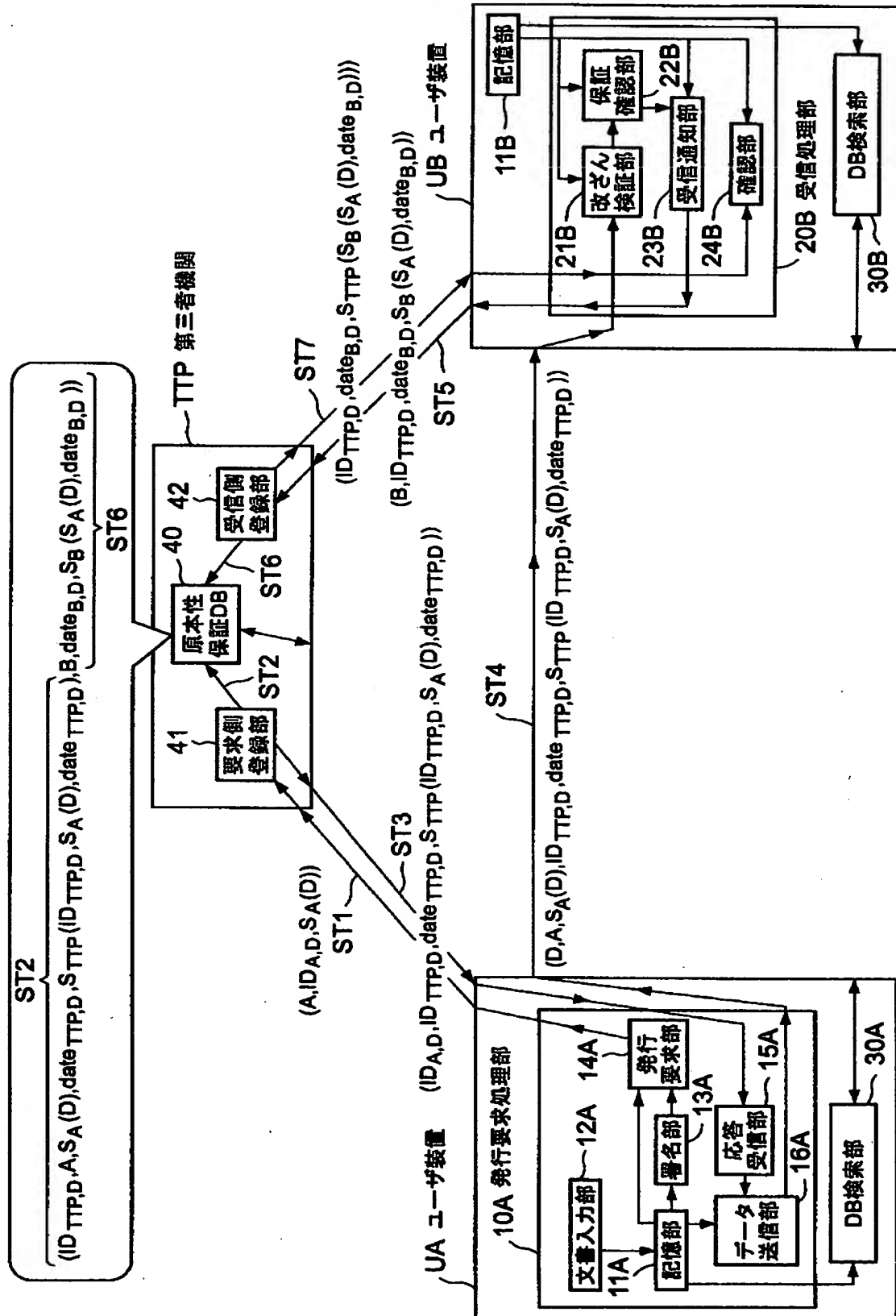
【書類名】

図面

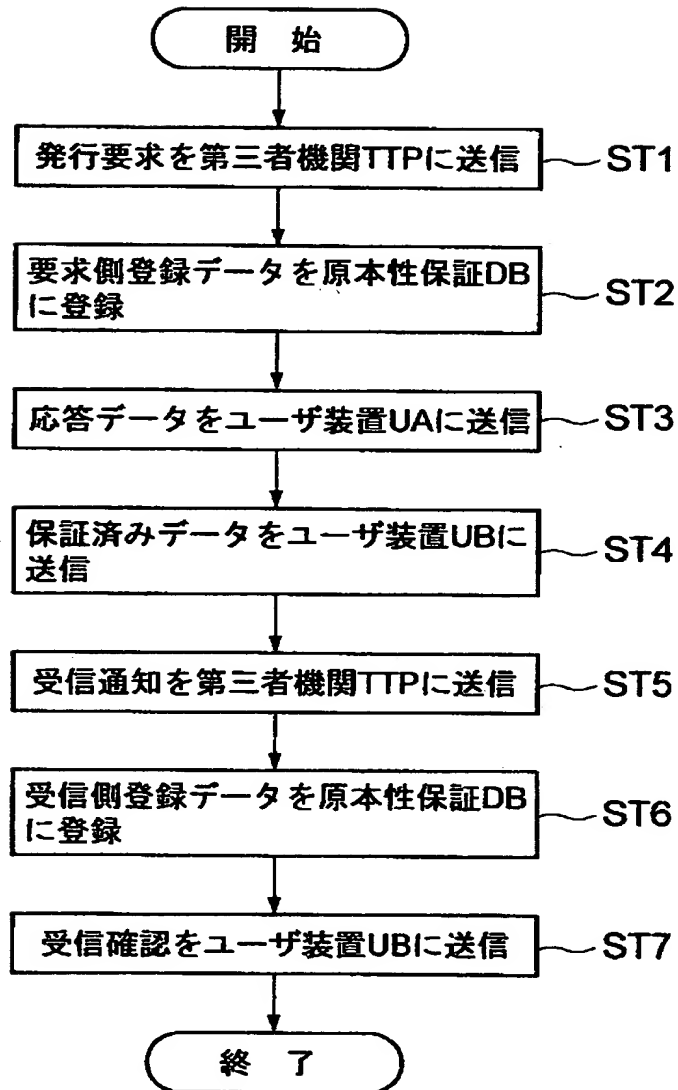
【図 1】



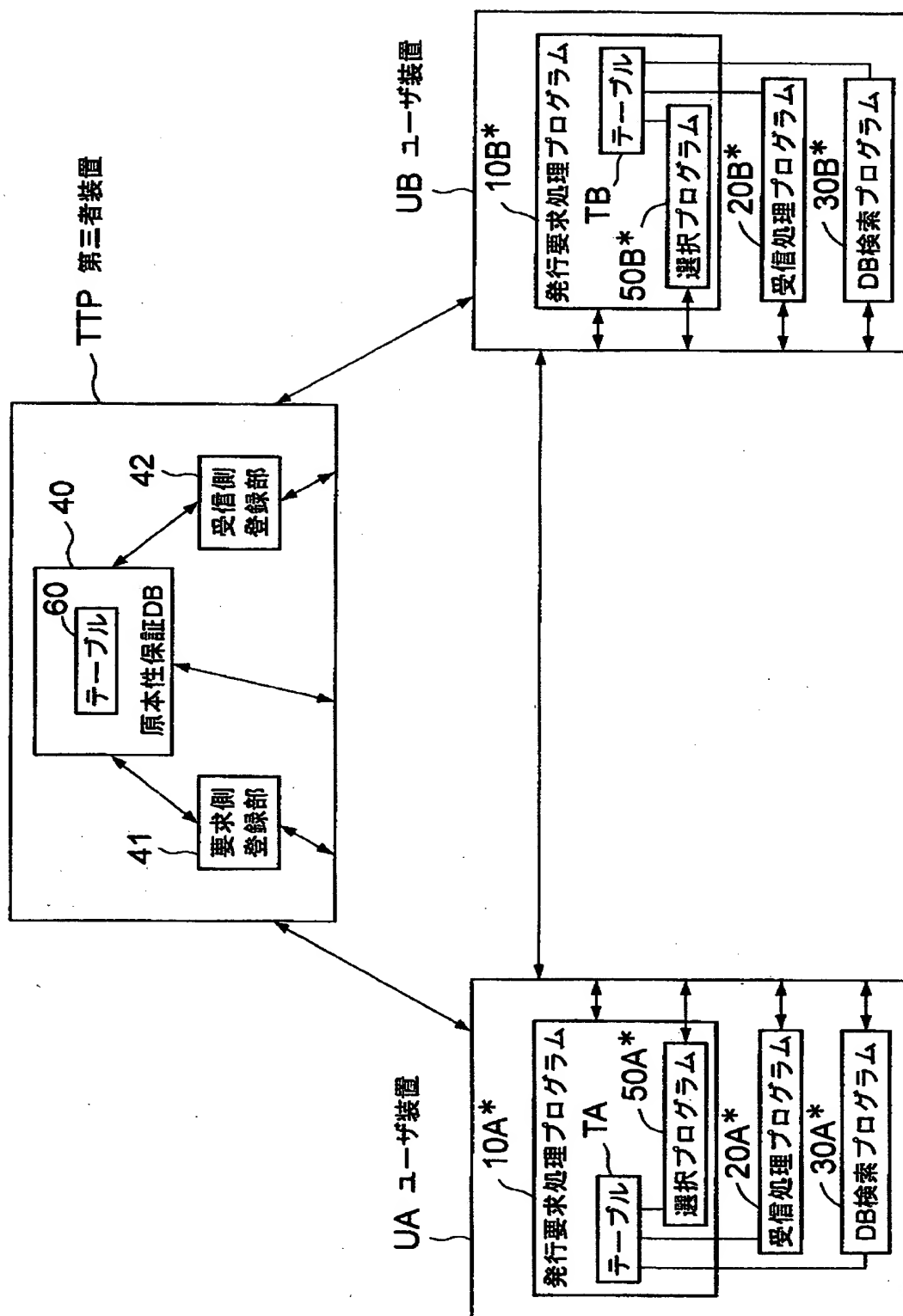
【図 2】



【図3】



【図4】



【図5】

60

A	P _A	ADR _A	ftp
B	P _B	ADR _B	smtp
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

【図6】

TA

(a)

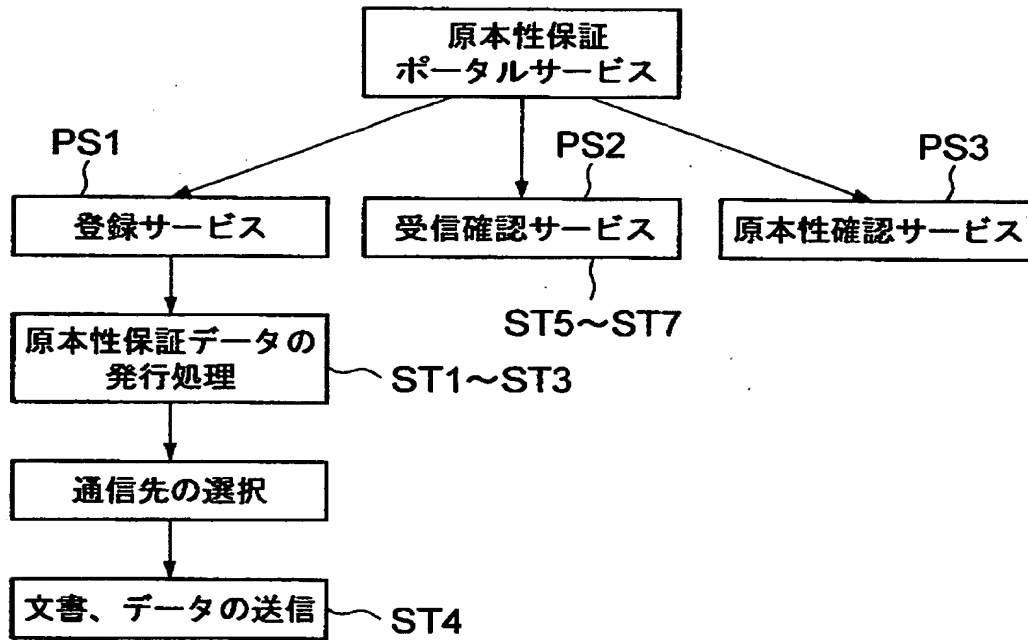
TTP	P _{TTP}	ADR _{TTP}	ftp
B	P _B	ADR _B	smtp
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

TB

(b)

TTP	P _{TTP}	ADR _{TTP}	ftp
A	P _A	ADR _A	ftp
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮

【図 7】



【書類名】 要約書

【要約】

【課題】 第三者機関やその間のネットワークにかかる負荷を低減させる。

【解決手段】 電子化文書Dに対するユーザ装置UAの電子署名 $S_A(D)$ に対し、第三者機関TTPの発行した時刻情報 $date_{TTP}$ を付与し、これら電子署名と時刻情報の組に対して第三者機関の電子署名を施すことにより、電子化文書の原本性を保証する。これによれば、電子化文書の原本性保証の際に、第三者機関装置には電子化文書が送信されないので、第三者機関装置にアクセスが集中した際にも、第三者機関やその間のネットワークにかかる負荷を低減できる。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日
[変更理由] 新規登録
住 所 神奈川県川崎市幸区堀川町72番地
氏 名 株式会社東芝
2. 変更年月日 2001年 7月 2日
[変更理由] 住所変更
住 所 東京都港区芝浦一丁目1番1号
氏 名 株式会社東芝